Аналитический обзор

инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств

(первое полугодие 2013)

2013

Содержание

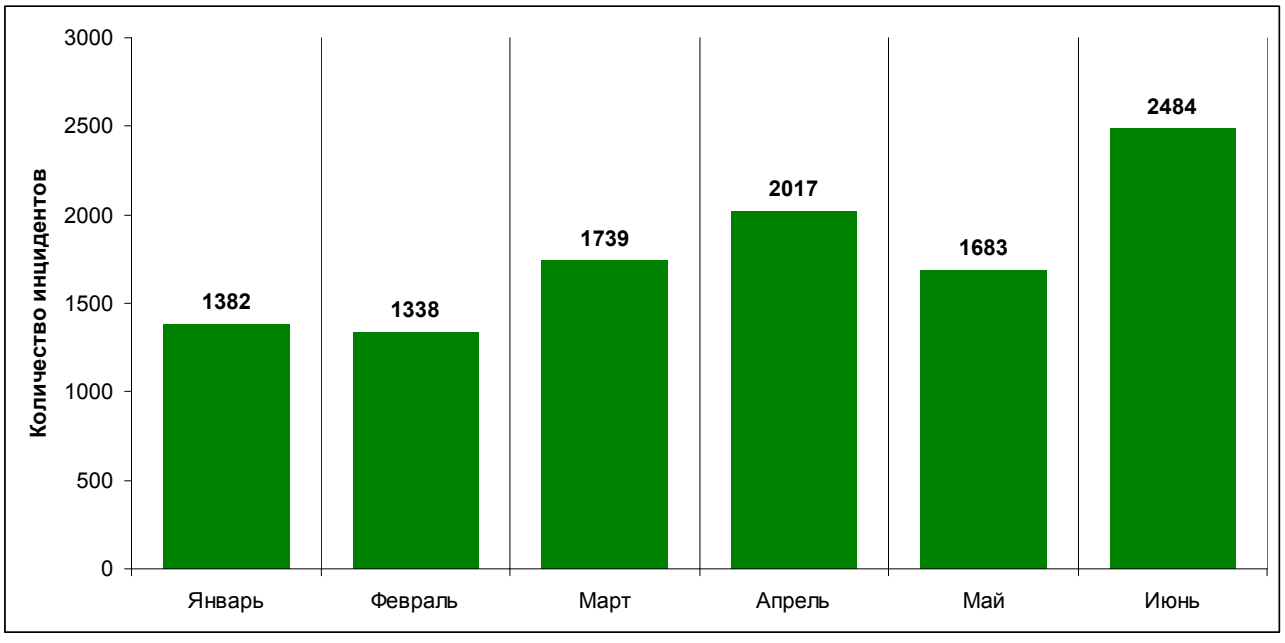
1. Общее описание ситуации
Вводная часть

Обзор подготовлен на основании отчетности по форме 0403203 «Сведения о выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств», предоставленной в Банк России операторами по переводу денежных средств, операторами услуг платежной инфраструктуры *(далее – отчитывающиеся операторы)* в соответствии с Указанием Банка России от 09.06.2012 № 2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств» в первом полугодии 2013 года (далее – анализируемый период).

1.1. Количество выявленных инцидентов

Динамика общего количества инцидентов представлена на рисунке 1:

Рисунок 1. Количество инцидентов



Сопоставление с данными за второе полугодие 2012 года позволяет сделать вывод о сохранении тенденции увеличения количества инцидентов в период с июля 2012 года по июнь 2013 года.

1.2. Распределение по количеству инцидентов, выявляемых одним оператором.

Динамика доли операторов, не выявивших инцидентов, приведена в таблице 1. Количество отчитывающихся операторов, не выявивших инцидентов, практически не изменилось по сравнению со вторым полугодием 2012 года.

Таблица 1. Динамика доли операторов, не выявивших инцидентов

	январь	**февраль**	**март**	**апрель**	**май**	**июнь**
Доля операторов, не выявивших инциденты, в общем количестве операторов	90%	89%	90%	89%	88%	87%

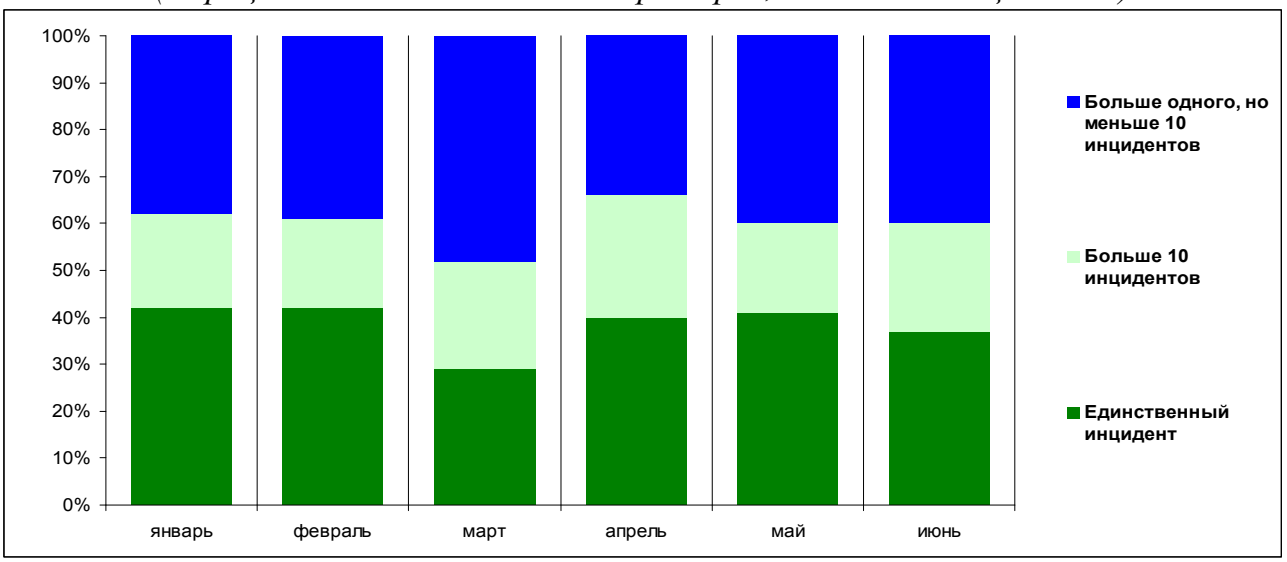
Распределение операторов, сообщивших о выявлении инцидентов, по количеству инцидентов, приходящемуся на одного оператора, представлено в таблице 2:

Таблица 2. Распределение операторов, выявивших инциденты, по количеству инцидентов, приходящемуся на одного оператора (в процентах от общего количества операторов, выявивших инциденты)

	январь	**февраль**	**март**	**апрель**	**май**	**июнь**
Единственный инцидент	42%	42%	29%	40%	41%	37%
Больше одного, но меньше 10	38%	39%	48%	34%	40%	40%
Больше 10, но меньше 20	7%	7%	7%	11%	5%	6%
Больше 20, но меньше 50	6%	5%	8%	6%	7%	8%
Больше 50, но меньше 100	4%	4%	5%	5%	4%	7%
Больше ста инцидентов	3%	3%	3%	4%	3%	2%

Порядка 80% отчитывающихся операторов, выявивших инциденты, выявляют менее 10 инцидентов в месяц, при этом, от 29% до 42% операторов сообщают только об одном выявленном инциденте. Порядка 20% отчитывающихся операторов фиксируют более 10 инцидентов в месяц (рисунок 2).

Рисунок 2. Распределение операторов, выявивших инциденты, по количеству инцидентов, приходящемуся на одного оператора (в процентах от количества операторов, выявивших инциденты)



1.3. Распределение инцидентов по федеральным округам

Данные о распределении инцидентов по федеральным округам приведены в таблице 3 и на рисунке 3.

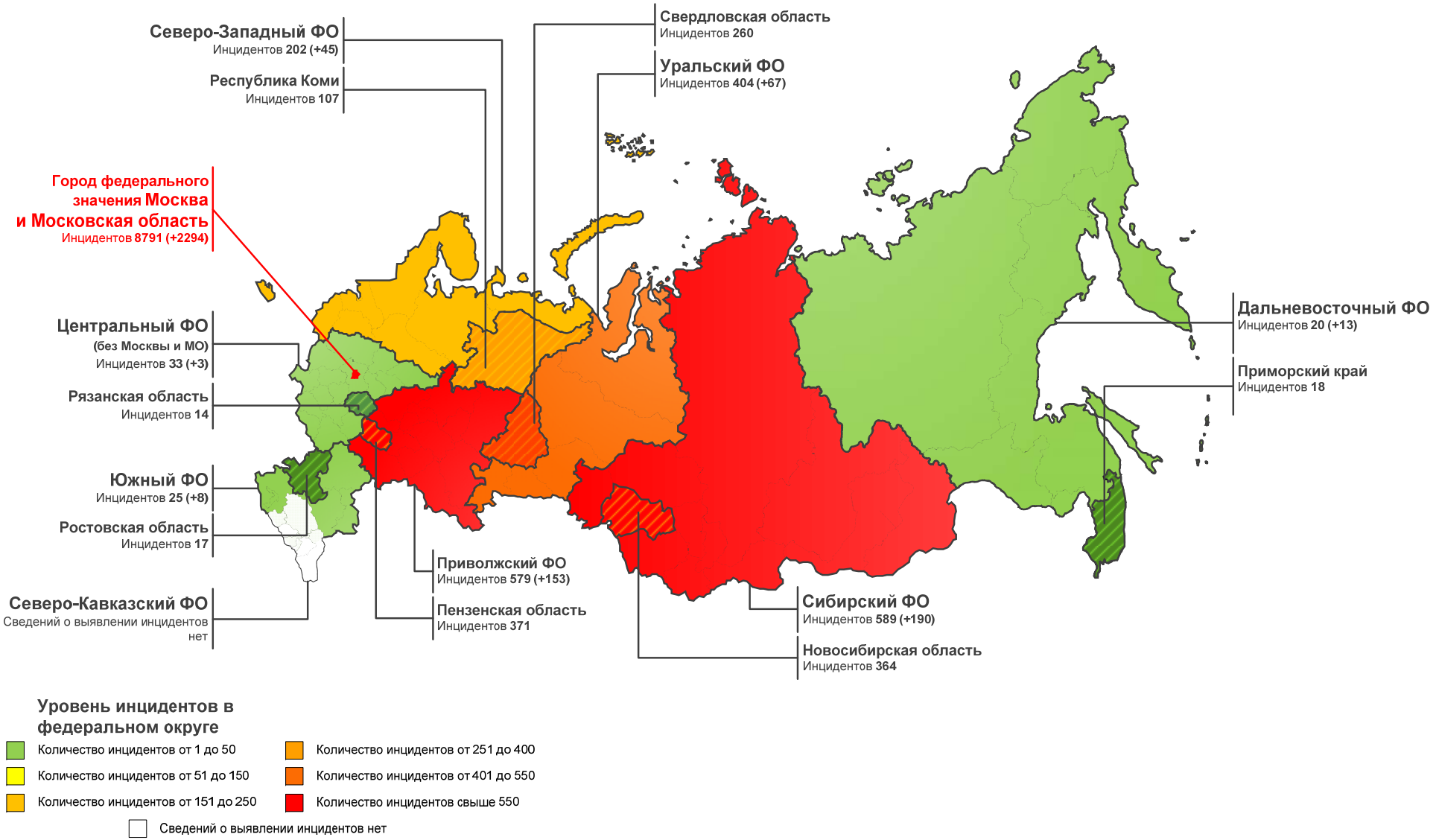
Таблица 3. Распределение инцидентов по федеральным округам

№ п/п	Федеральный округ	Количество инцидентов за полугодие (изменение по сравнению с предыдущим полугодием)	Прирост количества инцидентов за полугодие	Регион, в котором зафиксировано наибольшее количество инцидентов
1.	Город федерального значения Москва и Московская область	8791 (+2294)	35,31%	Москва и Московская область
2.	Сибирский федеральный округ	589 (+190)	38,26%	Новосибирская область
3.	Приволжский федеральный округ	579 (+153)	45,11%	Пензенская область
4.	Уральский федеральный округ	404 (+67)	19,88%	Свердловская область
5.	Северо-Западный федеральный округ	202 (+45)	28,66%	Республика Коми
6.	Центральный федеральный округ (без г. Москвы и области)	33 (+3)	10,00%	Рязанская область
7.	Южный федеральный округ	25 (+8)	47,06%	Ростовская область
8.	Дальневосточный федеральный округ	20 (+13)	185,71%	Приморский край

9.	Северо-Кавказский федеральный округ	0 (0)	0%	

За анализируемый период, по сравнению со вторым полугодием 2012 года, отмечается рост числа инцидентов во всех федеральных округах (за исключением Северо-Кавказского). Данная тенденция обусловлена, в том числе, и повышением качества составления отчетности отчитывающимися операторами.

Рисунок 3. Распределение инцидентов по федеральным округам



2. Динамика распределения количества инцидентов по видам их последствий и по объектам информационной инфраструктуры, на которых они были выявлены.

2.1. Общая информация

Указанием Банка России от 09.06.2012 №2831-У установлены классификаторы инцидентов двух типов: по типам их последствий и по типам объектов информационной инфраструктуры.

2.2. Распределение инцидентов по типам их последствий

Данные по распределению инцидентов по типам их последствий за анализируемый период времени приведены в таблице 4:

Таблица 4. Распределение инцидентов по типам их последствий, в процентах от общего количества инцидентов

Код последстви	Последствие инцидента	Доля в общем количестве инцидентов
1	Воздействие вредоносного кода, приводящее к нарушению штатного функционирования средства вычислительной техники, результатом которого является нарушение предоставления услуг по переводу денежных средств или несвоевременности осуществления переводов денежных средств.	0,4%
2	Реализация воздействий с целью создания условий невозможности предоставления услуг по переводу денежных средств или несвоевременности осуществления переводов денежных средств.	1,2%
3	Нарушение конфиденциальности информации, необходимой для удостоверения клиентами операторов по переводу денежных средств права распоряжения денежными средствами.	27,1%
4	Компрометация ключевой информации средств криптографической защиты информации, используемых при осуществлении переводов денежных средств.	7,5%
5	Осуществление переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами.	46,8%
6	Воздействие вредоносного кода, приводящее к осуществлению	4,4%

	переводов денежных средств с использованием искаженной информации, содержащейся в распоряжениях клиентов.	
7	Невозможность предоставления услуг по переводу денежных средств в платежной системе в течении трех часов и более.	12,6%

Распределения выявленных инцидентов по типам их последствий практически аналогично сложившемуся во втором полугодии 2012 года.

2.3. Распределение инцидентов по типам объектов информационной инфраструктуры

За анализируемый период доля инцидентов по типам объектов информационной инфраструктуры распределилась следующим образом (таблица 5):

Таблица 5. Распределение инцидентов по типам объектов информационной инфраструктуры, в процентах от общего количества инцидентов

Код объекта	**Объект информационной инфраструктуры**	**Доля в общем количестве инцидентов**
1	Автоматизированные системы, используемые для осуществления переводов денежных средств	22,2%
2	Программное обеспечение, используемое для осуществления переводов денежных средств	29,3%
3	Средства вычислительной техники, используемые для осуществления переводов денежных средств	40,8%
4	Телекоммуникационное оборудование, используемое для осуществления переводов денежных средств	1,9%
5	Технические средства по защите информации, используемые для осуществления переводов денежных средств.	5,8%

В описании объектов информационной инфраструктуры отчитывающиеся операторы в основном указывают системы дистанционного банковского обслуживания (в том числе на автоматизированном рабочем месте клиента), банкоматы и платежные терминалы, платежные карты.

3. Деятельность по повышению уровня защиты информации при осуществлении переводов денежных средств

Кредитные организации в целях обеспечения защиты информации при осуществлении переводов денежных средств и противодействия угрозам, указанным в настоящем обзоре, продолжают реализовывать комплекс мероприятий организационного и технического характера (основные мероприятия отражены в обзоре за второе полугодие 2012 года).

В целях снижения рисков нарушения защиты информации при осуществлении переводов денежных средств с использованием электронных средств платежа (включая системы дистанционного банковского обслуживания) подготовлены изменения в Положение Банка России от 09.06.2012 № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» в части установления требований:

— к обеспечению защиты информации при осуществлении переводов денежных средств с использованием банкоматов и платежных терминалов;

— к выпуску и обслуживанию платежных карт с микропроцессором;

— к обеспечению защиты информации при осуществлении переводов денежных средств с применением технологий Интернет-банкинга, мобильного банкинга, в том числе к удостоверению распоряжений клиентов с использованием одноразовых паролей.

В целях повышения качества предоставления сведений об инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, в Указание Банка России от 09.06.2012 № 2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств» внесены следующие изменения (вступят в силу с 28.01.2014):

- уточнен порядок предоставления сведений о причинах и условиях возникновения инцидентов, в том числе инцидентов, произошедших при использовании электронных средств платежа клиентами отчитывающихся операторов, а также о последствиях инцидентов, включая оценку в денежном выражении убытков, причиненных в результате их возникновения;

- уточнена классификация инцидентов с целью детализации сведений об инцидентах;

- добавлен раздел, предназначенный для предоставления отчитывающимися операторами сведений об инцидентах предыдущих отчетных периодов (по результатам проведенных разбирательств по факту возникновения инцидентов);

- установлена обязанность оператора платежной системы, привлекающего для оказания операционных услуг участникам платежной системы операционный центр, находящийся за пределами Российской Федерации, предоставлять отчетность, содержащую сведения об инцидентах, выявленных данным операционным центром.